#	Cite Type	Ref #	State	Area Examined	Violation Category	Violation Date	Cite Title	Category	Compliance	Detail	Issue
1	Regulation	23 NYCRR 500.15	NY	Company operations and management	Respondent failed to timely encrypt documents containing NPI as required by the Department's Cybersecurity Regulation. 23 NYCRR Section 500.15 requires, among other things, documents containing NPI be encrypted. While encryption would not have prevented the data exposure of NPI due to the Vulnerability, the encryption requirement of 23 NYCRR Section 500.15 went into effect on September 1, 2018 – 18 months after the Part 500 regulation went into effect. Nonetheless, Respondent did not encrypt the tens of millions of documents tagged as containing NPI until approximately December 2018, months after the relevant provisions of the Cybersecurity Regulation went into effect. , etc...	7/21/2020	Cybersecurity Requirements for Financial Services Companies (Refs & Annos) - Encryption of nonpublic information	Company Operations and Managemen t	Cybersecurity requirements	Encryption of nonpublic information	Failed to timely encrypt documents containing NPI as required by DOI
2	Regulation	23 NYCRR 500.2	NY	Company operations and management	Respondent failed to perform risk assessments for data stored or transmitted within its Information Systems, specifically the FAST and EaglePro applications, despite those applications' transmission and storage of NPI. Respondent's acts or practices, for the period beginning on the effective date of this Section, March 1, 2017, through May 24, 2019, constitute a violation of 23 NYCRR 500.02.	7/21/2020	Cybersecurity program	Company Operations and Managemen t	Cybersecurity requirements	Cybersecurity programs	Failed to maintain cybersecurity program to protect information system

#	Cite Type	Ref #	State	Area Examined	Violation Category	Violation Date	Cite Title	Category	Compliance	Detail	Issue
3	Regulation	23 NYCRR 500.3	NY	Company operations and management	Respondent failed to maintain and implement data governance and classification policies for NPI suitable to its business model and associated risks. Respondents classification of EaglePro as an application that did not contain or transmit NPI was incorrect given that EaglePro could and did allow access to documents containing NPI. Respondent did not maintain an appropriate, risk-based policy governing access controls for EaglePro. These inadequate access controls failed to prevent the exposure of NPI in millions of documents. Respondents acts or practices for the period beginning on the effective date of the Section, March 1, 2017, through May 24, 2019, constitute violations of 23 NYCRR 500.03.	7/21/2020	Cybersecurity policy	Company Operations and Management	Cybersecurity requirements	Cybersecurity policy requirements	Failed to maintain/implement data governance/classification policies
4	Regulation	23 NYCRR 500.7	NY	Company operations and management	Section 500.07 of the Cybersecurity Regulation, 23 NYCRR 500.07, requires that a Covered Entity shall limit user access privileges to Information Systems that provide access to NPI and shall periodically review such access privileges.The Vulnerability allowed unauthorized remote users to gain access to NPI in Respondent's FAST system. The Vulnerability existed due to a lack of reasonable access controls. Any person could access sensitive documents stored in FAST simply by altering an EaglePro URL. Respondent's acts or practices, for the period beginning on the effective date of the Section, March 1, 2017, through May 24, 2019, constitute a violation of 23 NYCRR 500.07.	7/21/2020	Access privileges	Company Operations and Management	Cybersecurity requirements	Access privileges	Failed to limit user access privileges that provide access to NPI

#	Cite Type	Ref #	State	Area Examined	Violation Category	Violation Date	Cite Title	Category	Compliance	Detail	Issue
5	Regulation	23 NYCRR 500.9	NY	Company operations and management	The Risk Assessment was not sufficient to inform the design of the cybersecurity program as required by 23 NYCRR Part 500, as indicated not only by Respondents failure to identify where NPI was stored and transmitted through its Information Systems, but also its failure to identify the availability and effectiveness of controls to protect NPI and Information Systems. Respondents acts or practices, for the period beginning on the effective date of this Section, March 1, 2018, through May 24, 2019, constitute a violation of 23 NYCRR 500.09.	7/21/2020	Risk assessment	Company Operations and Management	Cybersecurity requirements	Risk assessment requirements	Failed to inform design of cybersecurity program per 23 NYCRR Part 500
6	Regulation	23 NYCRR 500.14	NY	Company operations and management	Respondent did not provide adequate data security training for Respondents employees and affiliated title agents responsible for identifying and uploading sensitive documents into the FAST system and in using the EaglePro system. This failure was especially significant since both the process of identifying sensitive documents and the only control preventing NPI from being distributed through EaglePro depended solely on employees and users correctly identifying sensitive documents and treating them appropriately. As a result, Respondent did not adopt cybersecurity awareness training that reflected the risks inherent in its operations and led to the Vulnerability reported on May 24, 2019.	7/21/2020	Training and monitoring	Company Operations and Management	Cybersecurity requirements	Training and monitoring requirements	Failed to provide adequate data security training for employees agents

#	Cite Type	Ref #	State	Area Examined	Violation Category	Violation Date	Cite Title	Category	Compliance	Detail	Issue
7	Regulation	23 NYCRR 500.15	NY	Company operations and management	Until the end of 2018, Respondent failed to encrypt documents marked as sensitive within the FAST repository. Other documents that contained sensitive data but were erroneously not marked as sensitive– were not encrypted until mid-2019. Respondent did not implement controls suitable to protect the NPI stored or transmitted by it, both in transit over external networks and at rest, nor did Respondent implement suitable compensating controls approved by the CISO. Respondents acts or practices, for the period beginning on the effective date of the Section, September 1, 2018, through May 24, 2019, constitute a violation of 23 NYCRR 500.15.	7/21/2020	Cybersecurity Requirements for Financial Services Companies (Refs & Annos) - Encryption of nonpublic information	Company Operations and Management	Cybersecurity requirements	Encryption of nonpublic information	Failed to timely encrypt documents containing NPI as required by DOI

LOU PENN & Associates, Inc.
Market Conduct Auditor®

Call: 1-866-458-4333 or visit
www.MarketConductAuditor.com

Cybersecurity Requirements for Financial Services Companies - NYCRR Title 23, Ch. I, Pt. 500

Template for New York DOI Market conduct examination for compliance with their new cybersecurity regulation - **NYCRR Title 23, Ch. I, Pt. 500**

23 NYCRR 500.15 NY

COMPANY OPERATIONS AND MANAGEMENT

Failed to timely encrypt documents containing NPI as required by the Department's Cybersecurity Regulation. 23 NYCRR Section 500.15 requires, among other things, documents containing NPI be encrypted. While encryption would not have prevented the data exposure of NPI due to the Vulnerability, the encryption requirement of 23 NYCRR Section 500.15 went into effect on September 1, 2018 – 18 months after the Part 500 regulation went into effect. Nonetheless, did not encrypt the tens of millions of documents tagged as containing NPI until approximately December 2018, months after the relevant provisions of the Cybersecurity Regulation went into effect, etc...

23 NYCRR 500.2 NY

COMPANY OPERATIONS AND MANAGEMENT

Failed to perform risk assessments for data stored or transmitted within its Information Systems, despite those applications' transmission and storage of NPI. 's acts or practices, for the period beginning on the effective date of this Section, March 1, 2017, through May 24, 2019, constitute a violation of 23 NYCRR 500.02.

23 NYCRR 500.3 NY

COMPANY OPERATIONS AND MANAGEMENT

Failed to maintain and implement data governance and classification policies for NPI suitable to its business model and associated risks. s classification of as an application that did not contain or transmit NPI was incorrect given that could and did allow access to documents containing NPI. did not maintain an appropriate, risk-based policy governing access controls for. These inadequate access controls failed to prevent the exposure of NPI in millions of documents. s acts or practices for the period beginning on the effective date of the Section, March 1, 2017, through May 24, 2019, constitute violations of 23 NYCRR 500.03.

23 NYCRR 500.7 NY

COMPANY OPERATIONS AND MANAGEMENT

Section 500.07 of the Cybersecurity Regulation, 23 NYCRR 500.07, requires that a Covered Entity shall limit user access privileges to Information Systems that provide access to NPI and shall periodically review such access privileges. The Vulnerability allowed unauthorized remote users to gain access to NPI in ’s system. The Vulnerability existed due to a lack of reasonable access controls. Any person could access sensitive documents stored in simply by altering an URL’s acts or practices, for the period beginning on the effective date of the Section, March 1, 2017, through May 24, 2019, constitute a violation of 23 NYCRR 500.07.

23 NYCRR 500.9 NY

COMPANY OPERATIONS AND MANAGEMENT

The Risk Assessment was not sufficient to inform the design of the cybersecurity program as required by 23 NYCRR Part 500, as indicated not only by s failure to identify where NPI was stored and transmitted through its Information Systems, but also its failure to identify the availability and effectiveness of controls to protect NPI and Information Systems. s acts or practices, for the period beginning on the effective date of this Section, March 1, 2018, through May 24, 2019, constitute a violation of 23 NYCRR 500.09.

23 NYCRR 500.14 NY

COMPANY OPERATIONS AND MANAGEMENT

Did not provide adequate data security training for s employees and affiliated title agents responsible for identifying and uploading sensitive documents into the FAST system and in using the system. This failure was especially significant since both the process of identifying sensitive documents and the only control preventing NPI from being distributed through depended solely on employees and users correctly identifying sensitive documents and treating them appropriately. As a result, did not adopt cybersecurity awareness training that reflected the risks inherent in its operations and led to the Vulnerability reported on May 24, 2019.

23 NYCRR 500.15 NY

COMPANY OPERATIONS AND MANAGEMENT

Until the end of 2018, failed to encrypt documents marked as sensitive within the FAST repository. Other documents that contained sensitive data but were erroneously not marked as sensitive– were not encrypted until mid-2019. did not implement controls suitable to protect the NPI stored or transmitted by it, both in transit over external networks and at rest, nor did implement suitable compensating controls approved by the CISO. s acts or practices, for the period beginning on the effective date of the Section, September 1, 2018, through May 24, 2019, constitute a violation of 23 NYCRR 500.15.